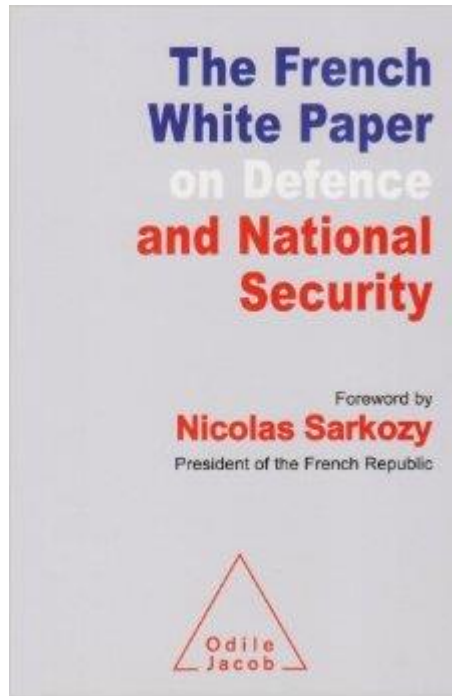


Resilience in Defense systems

Dominique Luzeaux

dominique.luzeaux@polytechnique.org

White papers on Defense and National Security (2008, 2013)



Resilience introduced, and defined as: “*the capability of public authorities and the French society to respond to a major crisis and rapidly restore normal functioning.*”



Resilience: issues

Organization

Societal + Political

Risk

Systems

Training



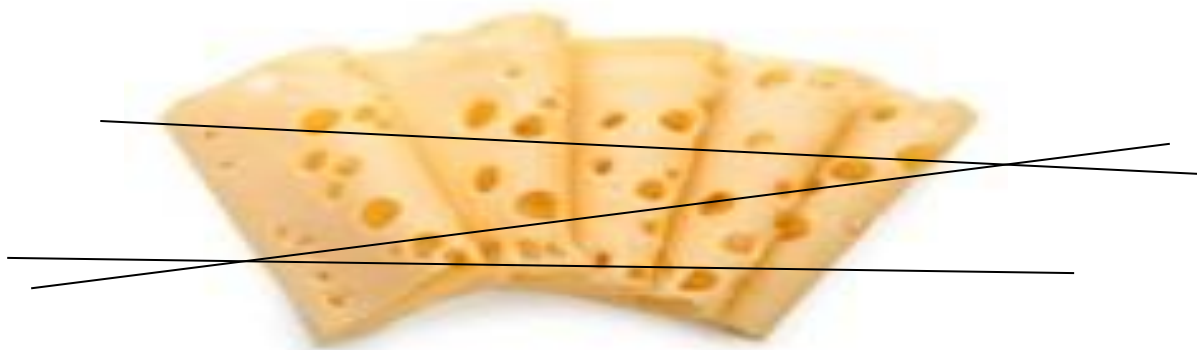
Cyber-resilience

[Joint Concept (FRA)JC-6.3 CYBERDEF, 2011]

- **Cyber-resilience:** capacity of an organization in strong symbiosis with its information system to pursue its mission as well as possible while containing and identifying the effects of a breakdown, especially coming from cyber-attacks.
- **Dynamic and in-depth defense:** rather than protection from an attack, the objective is to be able to identify the signs of an attack, to contain its effects and to stop it while keeping in mind that its form will probably evolve during the action, to plan and conduct operations for the full recovery of our capabilities.

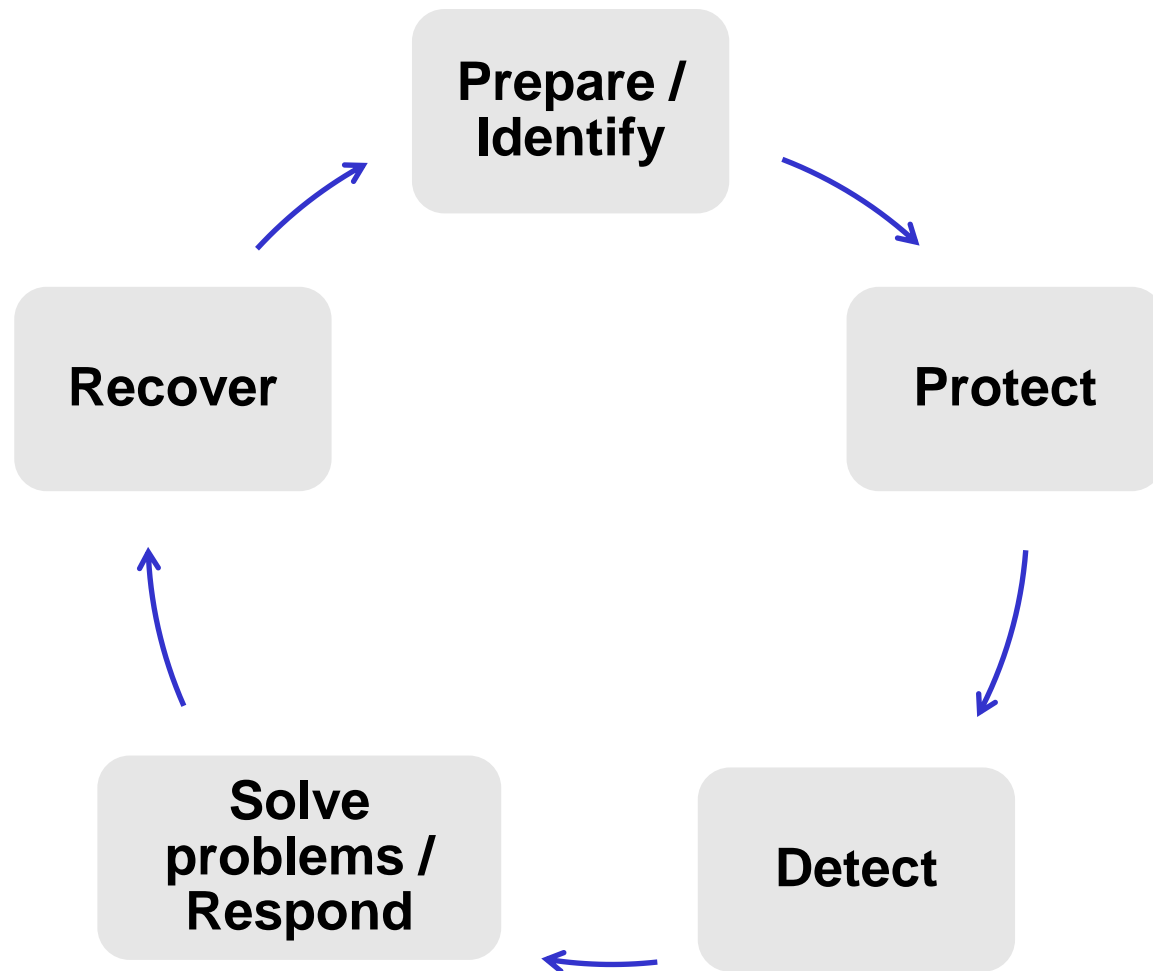
Cyber-resilience

- All components are not equally resilient (different initial states, different aptitudes to resist or recover).
- Manage security by adopting a multi-level approach, that encompasses: people, processes, technology.
- Multiple layers of defense: the Swiss cheese model.





Cyber-resilience



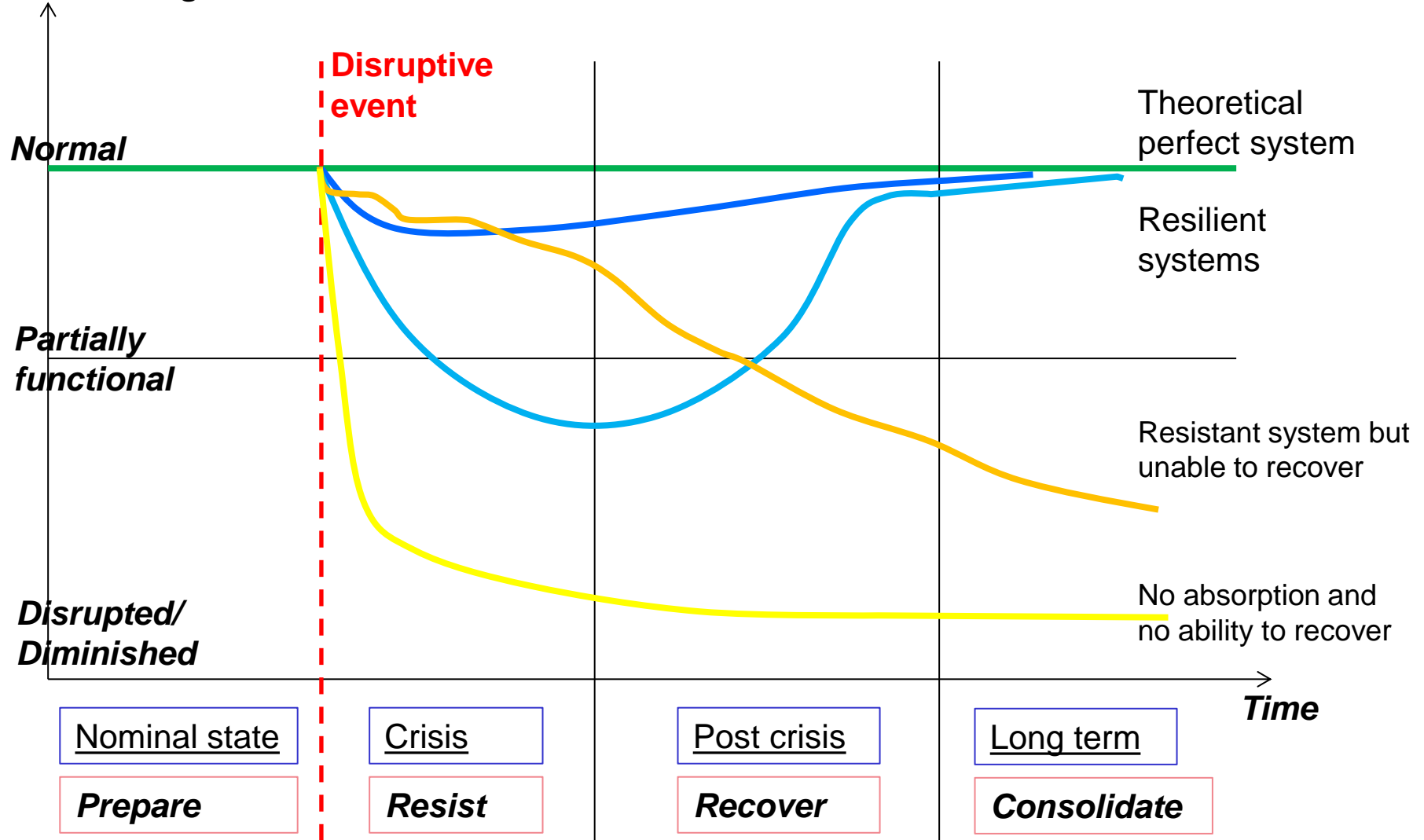


Manage cyber-resilience successfully


- Develop a strategy of resilience rather than hoping to suppress all risks:
 - cultural change.
- Train people and organizations: virtual exercises (war gaming) + regular exercises involving command structures (supplemented by participation in inter-ministerial exercises of national or international range).
- Favor a strategy that:
 - integrates *preparation, detection, response, recovery,*
 - focuses on *people, processes and technology,*
 - does not try to control everything.

► Typology of systems

Functioning states

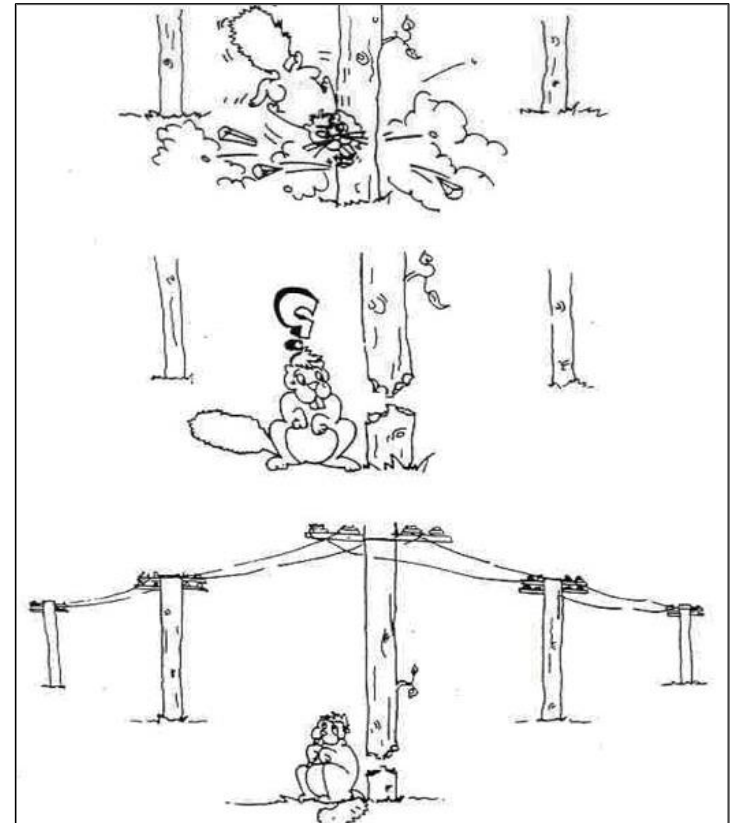
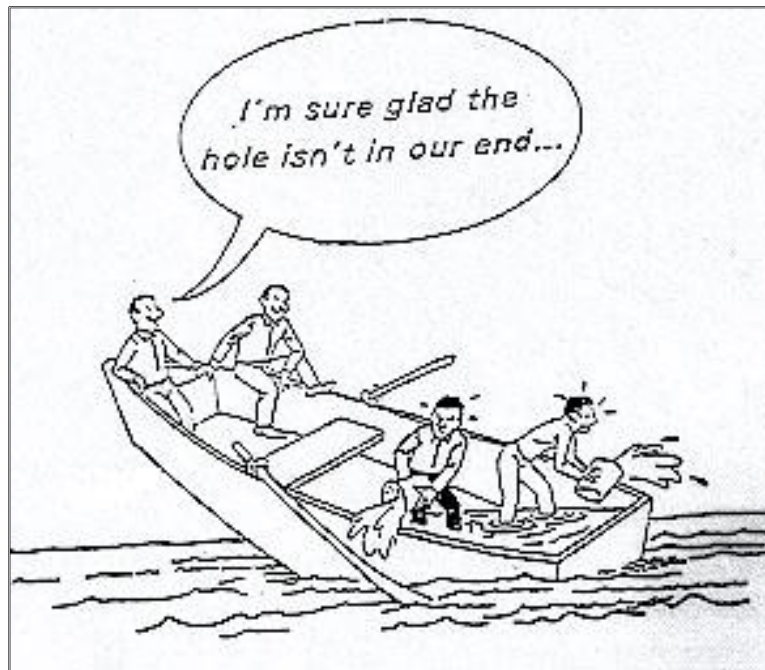


▶ Defense systems-of-systems: increasing complexity

- 
- **Structural complexity:** number of dependencies, of stakeholders, size, resource uncertainty.
 - **Technical complexity:** technical or design innovation, required technical maturity.
 - **Temporal complexity:** duration, shifting environmental and strategic directions, politics.
 - **Directional complexity:** number of unshared goals, ambiguity, stakeholders with differing positions.

► Resilience and systems theory

- **Function:** goal of resilience is to retain or restore as much of the function as possible.
- Understanding function/form needs **System thinking:**
Interaction – Holism – Hierarchy – Emergence – Nonlinearity.





Systems and disturbances

Robustness of graphs with different kinds of disturbances:

	Scale-free graph <i>(air traffic routes)</i>	Random graph <i>(road networks)</i>
Targeted attacks	Impact from weak to important (few attacks necessary)	Weak impact
Random attacks	Generally weak impact	More or less weak impact (depending on number of attacks)

Know / design your (infrastructure) network topology!

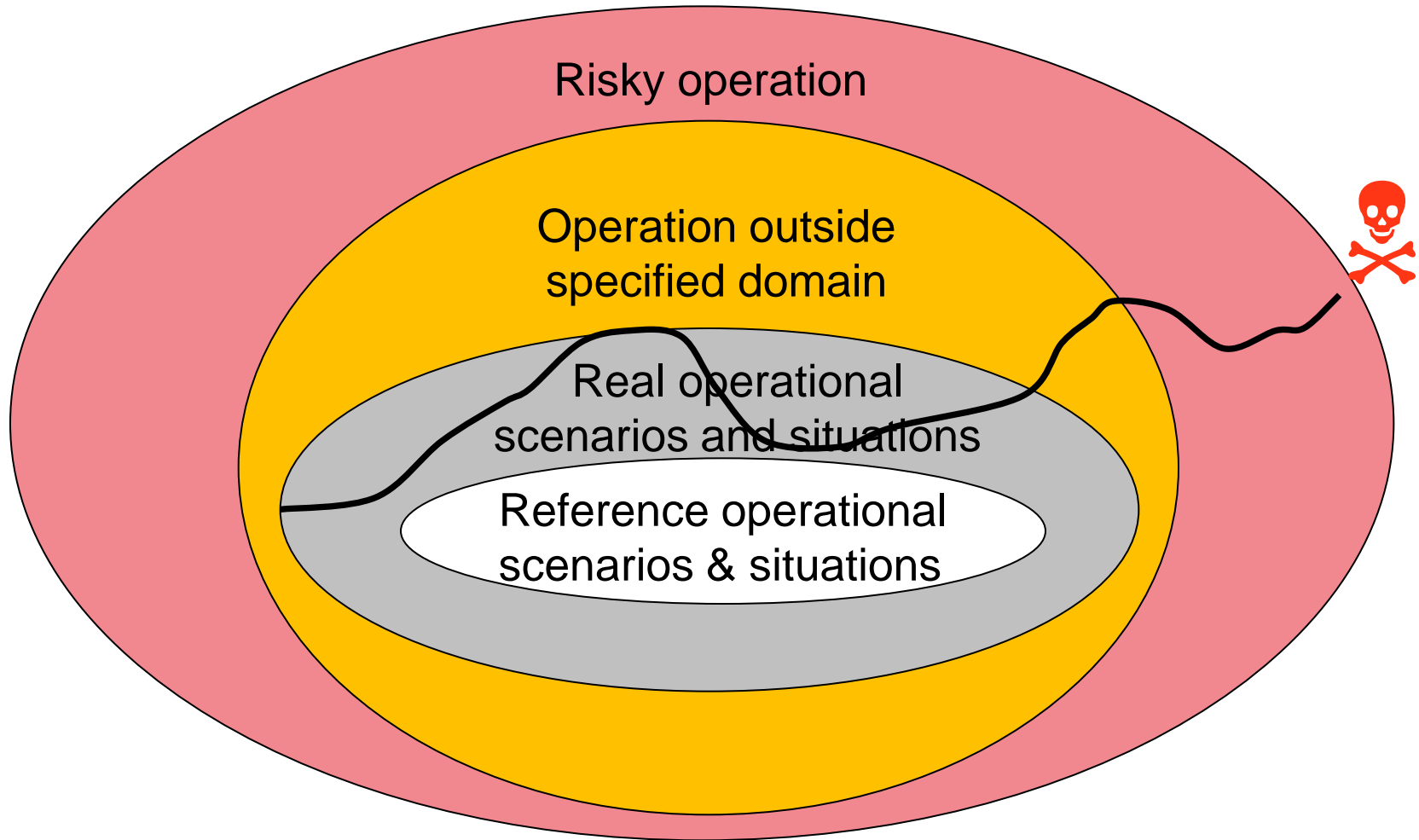


Resilience and systems theory

- **Control**: restore partial or full control of functionality.
- **Viability**: ability to live/survive under certain conditions.
- **Requisite variety** (Roger Conant, Ross Ashby):
 - Necessity for variation and flexibility within a system (to successfully regulate the outcome).
 - Too little system variety: stagnation, rigidity.
 - Too little regulatory variety: overload, instability, dependence.
- Systems-of-systems: legacy / new / interconnection...



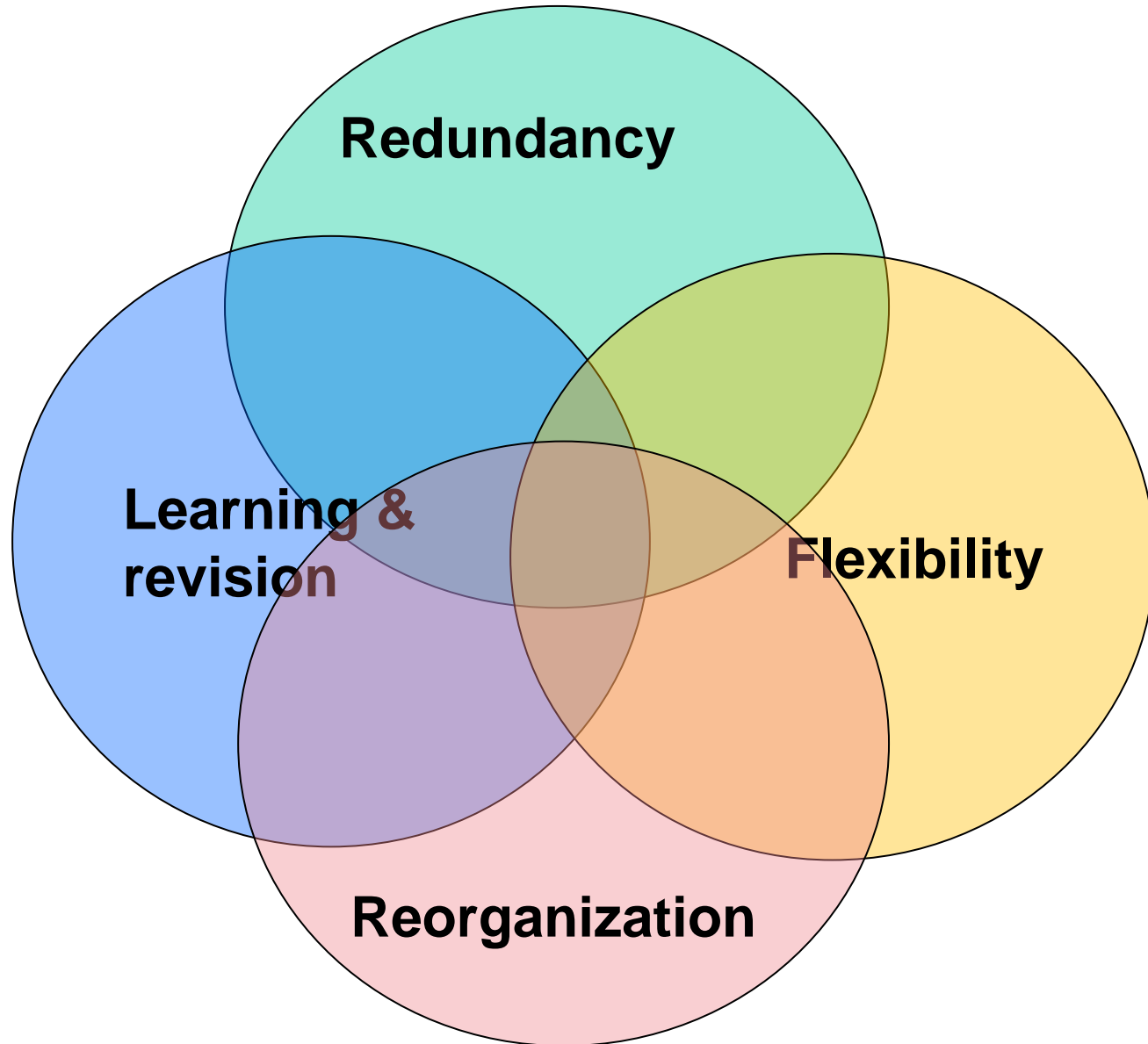
From control to viability



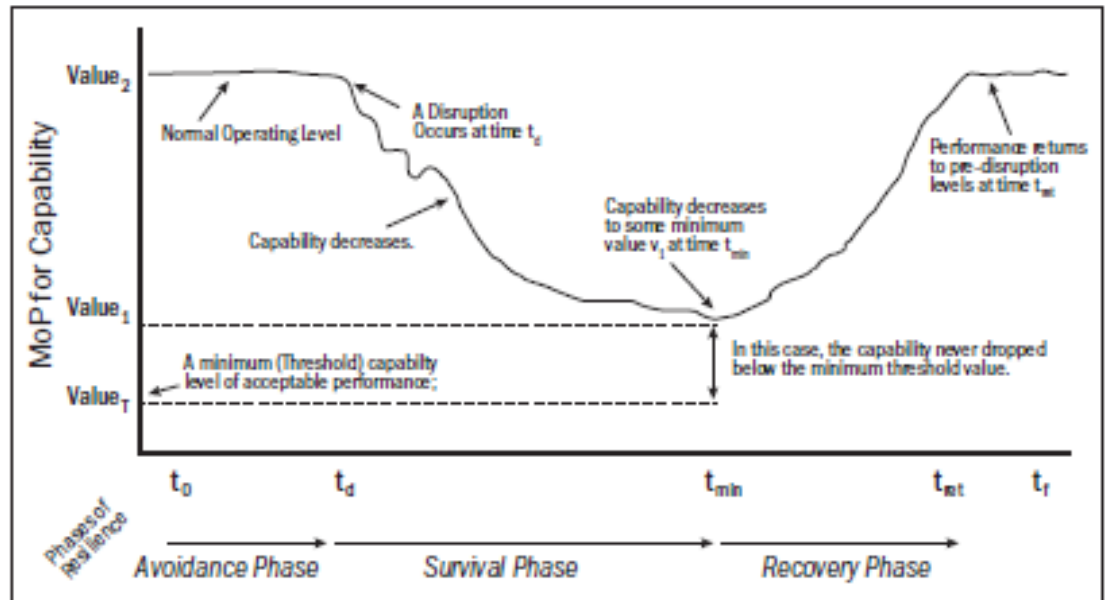


Resilient system architecting

- Good: technically sound.
- Right: meets stakeholders goals and fits contexts and purpose.
- Successful: actually delivers strategic outcomes.



Attributes of resilience and measure



- *Tolerance* = ability to degrade gracefully.
- *Effectiveness*: comparing performance with requirements.
- *Flexibility*: ability to reorganize its elements to maintain its capabilities and adapt to changing conditions.
- *Capacity*: available margins between current operating levels and minimum threshold operating level.
- **MoPs, MoEs...**



Conclusion (1/2)



Engineered robustness

Static

Reactive

Resist and reduce return-time-to-normal-conditions

Absorption and resistance capacity

Stable equilibrium

Systemic resilience

Dynamic

Proactive

Adapt to changing and unforeseen conditions
Reduce negative impacts, take advantage of opportunities

Adaptation, transformation, learning capacity

Bifurcations, multiple equilibria

Look for capability satisfaction more than permanent total control: *think like a gardener not a watch-maker.*



Conclusion (2/2)

- Resilience is an **individual** and a **collective** issue.
- Resilience is a **human** (*soft sciences*) as well as a **technical** (*hardware/software, hard sciences*) issue.
- Necessity of a new **culture of resilience** (based on risk & capacity management rather than performance control).
- Such a culture has to **disseminate** among political and defense/security circles AND the whole population (→ information, education, training).
- **Loss of resilience for a country would be potentially a total submission to the adversary.**